

EXAMEN UNIDAD 1 – EJERCICIO NMAP

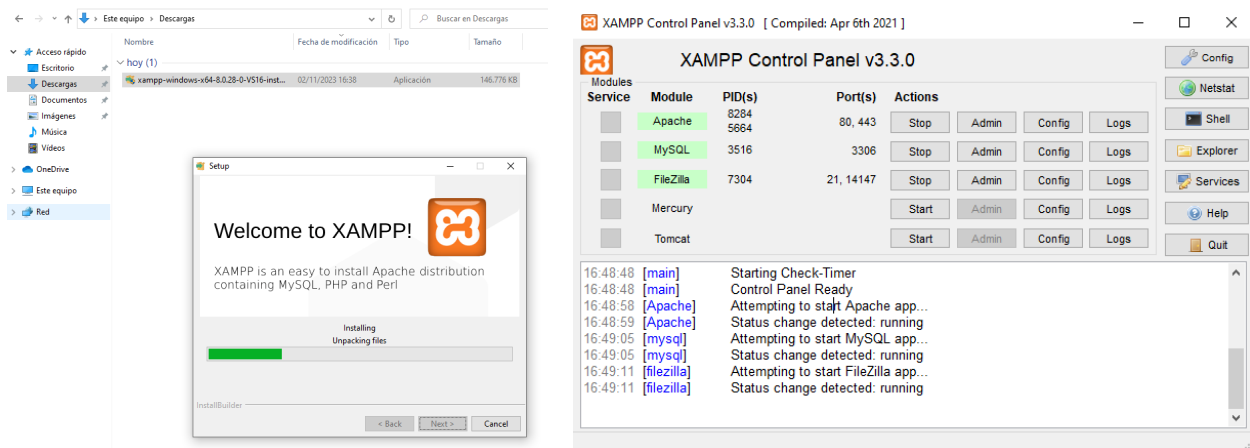
2º SMR – IES RAMÓN M.^a ALLER ULLOA

Nicolás González Dobarro

Índice

1. Instala XAMPP en Windows e inicia los servidores Apache, MySQL y FileZilla.....	3
2. Escanea la máquina Windows desde Ubuntu con NMAP (usando la interfaz de consola).....	3
1. Identifica qué servicios están disponibles en la máquina Windows.....	3
2. ¿Cuáles son las versiones de los servicios activos?.....	3
3. Ejecuta las opciones adecuadas para identificar el sistema operativo de la máquina objetivo..	5
3. Escanea desde Windows toda la red con NMAP (usando la interfaz gráfica) para comprobar los hosts activos.....	6
1. Muestra la imagen de toda la red.....	6

1. Instala XAMPP en Windows e inicia los servidores Apache, MySQL y FileZilla.



2. Escanea la máquina Windows desde Ubuntu con NMAP (usando la interfaz de consola).

1. Identifica qué servicios están disponibles en la máquina Windows.

Usamos el comando `nmap -sV 172.16.224.4` (IP cliente Windows) y nos proporciona todos los servicios con sus respectivas versiones que están corriendo en Windows.

```
root@usuario: /home/nicolas# nmap -sV 172.16.224.4
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-02 16:50 CET
Nmap scan report for 172.16.224.4
Host is up (0.00023s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          FileZilla ftpd 0.9.41 beta
80/tcp    open  http         Apache httpd 2.4.56 ((Win64) OpenSSL/1.1.1t PHP/8.0.28)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
443/tcp   open  ssl/http     Apache httpd 2.4.56 ((Win64) OpenSSL/1.1.1t PHP/8.0.28)
445/tcp   open  microsoft-ds?
3306/tcp  open  mysql        MariaDB (unauthorized)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:CD:F6:0A (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.64 seconds
root@usuario: /home/nicolas#
```

2. ¿Cuáles son las versiones de los servicios activos?

El comando utilizado es el mismo que el del ejercicio anterior.

```
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          FileZilla ftpd 0.9.41 beta
80/tcp    open  http         Apache httpd 2.4.56 ((Win64) OpenSSL/1.1.1t PHP/8.0.28)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
443/tcp   open  ssl/http     Apache httpd 2.4.56 ((Win64) OpenSSL/1.1.1t PHP/8.0.28)
445/tcp   open  microsoft-ds?
3306/tcp  open  mysql        MariaDB (unauthorized)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

3. Ejecuta las opciones adecuadas para identificar el sistema operativo de la máquina objetivo.

Utilizamos el comando `nmap -O 172.16.224.4`, en el cual `-O` es el parámetro para comprobar el sistema operativo de dicha IP. No nos proporciona ningún S.O. debido a un error porque tiene muchas etiquetas.

```
root@usuario: /home/nicolas

root@usuario:/home/nicolas# nmap -O 172.16.224.4
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-02 16:52 CET
Nmap scan report for 172.16.224.4
Host is up (0.00024s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
5357/tcp  open  wsddapi
MAC Address: 08:00:27:CD:F6:0A (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=11/2%OT=21%CT=1%CU=41655%PV=Y%DS=1%DC=D%G=Y%M=080027%T
OS:M=6543C5BD%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10D%TI=I%CI=I%II=I
OS:%SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M
OS:5B4NW8NNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70
OS: )ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=N%Q= )T1(R=Y%DF=Y%T=80%S=0%A=S+
OS:%F=AS%RD=0%Q= )T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q= )T3(R=Y%DF=Y%T
OS:=80%W=0%S=Z%A=0%F=AR%O=%RD=0%Q= )T4(R=Y%DF=Y%T=80%W=0%S=A%A=0%F=R%O=%RD=0
OS:%Q= )T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q= )T6(R=Y%DF=Y%T=80%W=0%S
OS:=A%A=0%F=R%O=%RD=0%Q= )T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q= )U1(R
OS:=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:%T=80%CD=Z)

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.41 seconds
root@usuario:/home/nicolas#
```

3. Escanea desde Windows toda la red con NMAP (usando la interfaz gráfica) para comprobar los hosts activos.

1. Muestra la imagen de toda la red.

Usamos el comando `nmap -T4 -F 172.16.224.0/24`, indicando la dirección de red y máscara para que nos muestre todos los equipos encendidos de esa red. Podemos observar que están disponibles el 172.16.224.2 y 172.16.224.4, los cuales son Ubuntu y Windows respectivamente.

Zenmap

Scan Tools Profile Help

Target: 172.16.224.0/24 Profile: Scan

Command: nmap -T4 -F 172.16.224.0/24

OS	Host
🌐	localhost (127.0.0.1)
🌐	172.16.224.1
🌐	172.16.224.2
🌐	172.16.224.3
🌐	172.16.224.4
🌐	172.16.224.5

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -F 172.16.224.0/24

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-02 16:56 Hora estándar romance
Nmap scan report for 172.16.224.1
Host is up (0.00051s latency).
Not shown: 99 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 172.16.224.2
Host is up (0.0010s latency).
Not shown: 97 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind
631/tcp   open  ipp
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 172.16.224.3
Host is up (0.0010s latency).
All 100 scanned ports on 172.16.224.3 are in ignored states.
Not shown: 100 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:61:1D:0B (Oracle VirtualBox virtual NIC)

Nmap scan report for 172.16.224.5
Host is up (0.00051s latency).
All 100 scanned ports on 172.16.224.5 are in ignored states.
Not shown: 100 closed tcp ports (reset)
MAC Address: 08:00:27:3C:EA:1E (Oracle VirtualBox virtual NIC)

Nmap scan report for 172.16.224.4
Host is up (0.000014s latency).
Not shown: 92 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
5357/tcp  open  wsddapi

Nmap done: 256 IP addresses (5 hosts up) scanned in 2.11 seconds
```